On the general theory of Möbius inversion formula and Möbius product

By RICHARD WIEGANDT in Orosháza (Hungary)

1. Introduction

The number-theoretic Möbius function and inversion formula (or Dedekind inversion formula) were generalized by DELSARTE [1], WARD [4], and WEISNER [5]. The most general results are in the cited paper of WARD. WARD defined the Möbius (or Dirichlet) product of functions defined for finite intervals of a partially ordered set. (An interval or quotient of a partially ordered set is a subset with elements d satisfying the relation $a \leqq d \leqq b$ for some elements a, b of the considered set.) WARD defined the Möbius function for intervals, and he got a generalization of the Möbius inversion formula. WARD's results include WEISNER's results. DELSARTE generalized the Möbius product and inversion formula to functions defined on the lattice of the subgroups of Abelian groups. Applications to the theory of groups and Abelian groups are given by WEISNER [5] and DELSARTE [1], respectively. A very interesting application of the Delsarte—Möbius inversion formula is in the theory of the group-theoretic ζ-functions introduced by L. RÉDEI [2], [3].

In this paper we consider an arbitrary partially ordered set. Assume that for every element a of the set the relation $d \leqq a$ has only a finite number of solutions in the set. In section 2 we define the sum and inversion function of a function defined on this set, and give a generalization of the Möbius inversion formula. The Möbius function appearing in the inversion formula is also a function of one variable defined on the set. If the considered set has only one minimal element, then these results may be obtained also from WARD [4]. In section 3 we define the Möbius product of functions defined on the considered set, and establish a necessary and sufficient criterion for the associativity and commutativity of the Möbius product, further we give the functions which have an inverse according to the Möbius product. In section 4 we demonstrate how we get the classical number-theoretic results and the results of DELSARTE from our theory. In section 5 we consider the partially ordered set of finite subsets of any countable set. Further specializing our theory, in this case we obtain simple inversion formulae which are applied in the probability and in coloring-theory.

2. Möbius function and inversion formula

Let S be an arbitrary partially ordered set in which the ordering relation is denoted by the sign $<$. If $a \leqq b$ $(a, b \in S)$ is valid, then we say that a is less than or equal to b. Assume that for every element $a\,(\in S)$ the relation $d \leqq a$ has only a finite number of solutions in S. By a set we understand throughout this paper a partially ordered set of this type.

Throughout this section denote by f and F functions defined on the set S, with values belonging to a given module.

Definition 1. By the sum function of a function f we understand the function

$$F(a) = \sum_{d \leqq a} f(d). \tag{1}$$

The function f is called the inversion function of the function F.

Theorem 1. *Every function F has an inversion function. The inversion function is determined uniquely by its sum function, namely*

$$f(a) = \sum_{d \leqq a} c_{ad} F(d) \qquad (a \in S) \tag{2}$$

is valid, where the coefficients c_{ad} are integers determined by the set S.

Proof. Let a be an arbitrary element of S. Order the elements less than a and the element a into a sequence such that any element of the sequence be not less than the preceding elements. Obviously this is possible. Let the considered sequence be

$$a_1, a_2, \ldots, a_n = a.$$

Writing up $F(a_i)$ for every $i\,(i = 1, \ldots, n)$ we get

$$F(a_i) = \sum_{k=1}^{n} \vartheta_{ik} f(a_k) \tag{3}$$

where

$$\vartheta_{ik} = \begin{cases} 1 & \text{if } \; a_k \leqq a_i, \\ 0 & \text{otherwise.} \end{cases}$$

Equations (3) form a system of linear equations in the unknowns $f(a_i)$. This system of equations may be solved by CRAMER's formula, since its determinant is the expression

$$D=|\vartheta_{ik}|=\begin{vmatrix} 1 & 0 & \cdot & \cdot & \cdot & 0 \\ \cdot & 1 & & & & \cdot \\ \cdot & & \cdot & & & \cdot \\ \cdot & & & \cdot & & \cdot \\ \cdot & & & & \cdot & 0 \\ \vartheta_{n1} & \cdot & \cdot & \cdot & \cdot & 1 \end{vmatrix}=1.$$

Thus (3) determines $f(a)$ uniquely, and $f(a)$ is a linear expression of values $F(a_i)$ $(i=1,\ldots,n)$, whose coefficients are integers determined by the set S. Thus Theorem 1 is proved.

The coefficients c_{ad} $(d\leqq a;\ a,d\in S)$ in (2) may be expressed in certain cases by the values of the Möbius function defined below.

Let $$\delta(a)=\begin{cases} 1 & \text{if } a \text{ is a minimal element of } S, \\ 0 & \text{otherwise} \end{cases}$$

(the so-called Dirac function).

Definition 2. The inversion function of the Dirac function δ is called the Möbius function defined on the set S, and it will be denoted by μ.

As a consequence of Definitions 1, 2 we have

$$\sum_{d\leqq a}\mu(d)=\delta(a) \qquad (a\in S).$$

By Theorem 1 the Möbius function exists, and it is uniquely determined.

It is easy to see that, if c_{ad} means the set of the non-negative integers which is partially ordered by the divisibility, then Definition 2 defines just the number-theoretic Möbius function.

Theorem 2. *The coefficients* c_{ad} *in* (2) *may be expressed as values of the Möbius function if and only if there exists a function* ϱ *of two variables defined on* S, *with values belonging to* S *such that for every elements* a,b $(b\leqq a;\ a,b\in S)$ *the equation*

$$(4) \qquad \sum_{b\leqq d\leqq a}\mu(\varrho(d,b))=\begin{cases} 1 & \textit{if } b=a, \\ 0 & \textit{otherwise} \end{cases}$$

is valid.

Proof. Assume that the coefficients in (2) may be expressed as values of the Möbius function. This means that for every elements a,b $(b\leqq a;$ $a,b\in S)$ there is an element $s\,(\in S)$ such that

$$(5) \qquad \mu(s)=c_{ab}$$

holds. Since s depends only on the elements a, b, so we have $s=\varrho(a, b)$ where ϱ means a function of two variables defined on S and with values belonging to S. Writing this expression of s into (5) we get

$$\mu(\varrho(a, b))=c_{ab}. \tag{6}$$

Substitute the values of f which are determined by the inversion formula (2) into the right-hand side of equation (1). We get

$$F(a)=\sum_{d\leqq a}\sum_{b\leqq d}c_{db}F(b).$$

Changing the summation variables we have

$$F(a)=\sum_{b\leqq a}F(b)\sum_{b\leqq d\leqq a}\mu(\varrho(d, b)).$$

Since by Theorem 1 this equality is an identity, so the equation

$$\sum_{b\leqq d\leqq a}\mu(\varrho(d, b))=\begin{cases}1 & \text{if } b=a,\\ 0 & \text{otherwise}\end{cases}$$

is valid proving the necessity of the condition.

Conversely, suppose that there exists a function which satisfies condition (4). Now the identity

$$F(a)=\sum_{b\leqq a}F(b)\sum_{b\leqq d\leqq a}\mu(\varrho(d, b))$$

holds. Changing the summation variables we get

$$F(a)=\sum_{d\leqq a}\sum_{b\leqq d}\mu(\varrho(d, b))F(b).$$

Hence $\sum_{b\leqq d}\mu(\varrho(d, b))F(b)$ is the inversion function of F, and by Theorem 1 it is uniquely determined. Thus we have

$$f(a)=\sum_{b\leqq d}\mu(\varrho(d, b))F(b).$$

This means that the coefficients in (2) may be expressed as values of the Möbius function, completing the proof.

Theorem 3 (general Möbius inversion formula). *If there exists a function ϱ defined on S which satisfies condition (4), then the equations*

$$\sum_{d\leqq a}f(d)=F(a) \qquad (a\in S),$$

$$\sum_{d\leqq a}\mu(\varrho(a, d))F(d)=f(a) \qquad (a\in S)$$

imply each other.

Theorem 3 is a simple consequence of Theorems 1 and 2.

On a set there may be defined sometimes more functions which satisfy condition (4). If ϱ and σ are two functions defined on S which fulfil condition (4), then by Theorem 3

$$\sum_{d \leqq a} \mu(\varrho(a, d)) F(d) = \sum_{d \leqq a} \mu(\sigma(a, d)) F(d) \qquad (a \in S)$$

is valid for every function F. This is possible only if

$$\mu(\varrho(a, b)) = \mu(\sigma(a, b))$$

holds for every elements a, b ($b \leqq a$; $a, b \in S$).

Conversely, there exist sets, on which no function satisfying condition (4) exists.

These assertions will be proved by the two following examples.

Example 1. Consider the set $S_1 = \{a, b, c, d, e\}$ with the partial ordering

$$a < b < e, \quad c < d < e.$$

It is easy to see that the values of the inversion function f of any function F are

$$f(a) = F(a), \quad f(c) = F(c),$$
$$f(b) = F(b) - F(a), \quad f(d) = F(d) - F(c),$$
$$f(e) = F(e) - F(b) - F(d) + 0 \cdot F(a) + 0 \cdot F(c);$$

and the values of the Möbius function are

$$\mu(a) = 1, \quad \mu(c) = 1,$$
$$\mu(b) = -1, \quad \mu(d) = -1,$$
$$\mu(e) = 0.$$

We see that in the expressions of the values of f, the coefficients of F may be substituted by the values of the Möbius function. So there exists a function defined on S_1 which fulfils condition (4). It is easy to see that there are more than one such functions.

Example 2. Consider the set $S_2 = \{a, b, c, d, e\}$ with the partial ordering

$$a, b < d; \quad b, c < e.$$

It is easy to see that the values of the inversion function f of any function F are

$$f(a) = F(a), \quad f(b) = F(b), \quad f(c) = F(c),$$
$$f(d) = F(d) - F(a) - F(b),$$
$$f(e) = F(e) - F(b) - F(c);$$

however, the values of the Möbius function are

$$\mu(a)=\mu(b)=\mu(c)=1, \quad \mu(d)=\mu(e)=-2.$$

We see that in the values of f, the coefficients of F may not be replaced by the values of the Möbius function, thus there does not exist any function defined on S_2 which fulfils condition (4).

3. Möbius product

In his cited paper DELSARTE defined the Möbius product of functions on finite Abelian groups. It is easy to generalize this definition to functions which are defined on any set S. For this aim consider the set $\mathfrak{F}$ of functions defined on the set S with values belonging to a given field. Let α be a function of two variables defined on S and with values belonging to S.

Definition 3. The Möbius product of two functions f, g ($\in \mathfrak{F}$) with respect to the function α (shortly their α-product) is the function

$$F(a)=f \overset{\circ}{\alpha} g=\sum_{d\leqq a} f(d)\, g(\alpha(a, d)) \qquad (a\in S).$$

The question arises under what conditions is the Möbius product associative and commutative. To examine this question we need the idea of factor-function.

Definition 4. A function α of two variables defined on the set S is called a factor-function, if it satisfies the conditions

a) $\alpha(a, b)\leqq a$ $\qquad (b\leqq a;\ a, b\in S)$,

b) $\alpha(a_1, b)<\alpha(a_2, b)$ $\qquad (b\leqq a_1<a_2;\ a_1, a_2, b\in S)$,

c) $\alpha(a, \alpha(a, b))=b$ $\qquad (b\leqq a;\ a, b\in S)$,

d) $\alpha(\alpha(a, c), \alpha(b, c))=\alpha(a, b)$ $\qquad (c\leqq b\leqq a;\ a, b, c\in S)$.

Theorem 4. *$\mathfrak{F}$ is a commutative semi-group with identity with respect to the α-product if and only if α is a factor-function. The Dirac function δ is the identity of $\mathfrak{F}$.*

In the proof of Theorem 4 we shall use some properties of the factor-functions. First we investigate these properties. Let α be any factor-function.

Property 1. If $\alpha(a, b_1)=\alpha(a, b_2)$ $(b_1, b_2\leqq a)$, then $b_1=b_2$.

Namely, using condition c) twice, we get

$$b_1=\alpha(a, \alpha(a, b_1))=\alpha(a, \alpha(a, b_2))=b_2.$$

Property 2. If $b_1 < b_2 \leqq a$ $(a, b_1, b_2 \in S)$, then $\alpha(a, b_1) > \alpha(a, b_2)$.

By condition $d)$

$$\alpha(a, b_2) = \alpha(\alpha(a, \alpha(b_2, b_1)), \alpha(b_2, \alpha(b_2, b_1)))$$

is valid. Using condition c) on the right-hand side we get

$$\alpha(a, b_2) = \alpha(\alpha(a, \alpha(b_2, b_1), b_1). \tag{6}$$

Since $b_2 \leqq a$, by condition b) we have $\alpha(b_2, b_1) \leqq \alpha(a, b_1)$, and so by condition a) $\alpha(b_2. b_1) \leqq a$. Using again condition a) we get $\alpha(a, \alpha(b_2, b_1)) \leqq a$. Thus applying condition b) for (6) we get

$$\alpha(a, b_2) \leqq \alpha(a, b_1).$$

Since $b_1 \neq b_2$, therefore by Property 1

$$\alpha(a, b_1) > \alpha(a, b_2)$$

is valid.

Property 3. In S, $\alpha(a, a)$ is the unique minimal element which is less than or equal to a.

Let a_0 be any minimal element of S, less than a. By condition c) we have

$$a_0 = \alpha(a, \alpha(a, a_0)) = \alpha(a, d)$$

where we have denoted the element $\alpha(a, a_0)$ by d. Since, by Property 2, $\alpha(a, a)$ is the least element among the elements $\alpha(a, d)$ $(d \leqq a)$, therefore

$$a_0 = \alpha(a, a)$$

holds necessarily.

For any two given elements a, b $(b \leqq a;\ a, b \in S)$ the set of elements d which satisfy the relation $b \leqq d \leqq a$, is called the interval $[b, a]$.

By Property 3 the elements less than or equal to a form exactly the interval $[a_0, a]$.

In the sequel let a_0 mean the element $\alpha(a, a)$.

Property 4. $\alpha(a, a_0) = a$.

Namely, using Property 3 and condition c), we get

$$\alpha(a, a_0) = \alpha(a, \alpha(a, a)) = a.$$

Property 5. The correspondence $d \longleftrightarrow \alpha(a, d)$ is a one-to-one mapping between the elements of intervals $[b, a]$ and $[a_0, \alpha(a, b)]$.

Property 1 implies that this correspondence is one-to-one. By Property 2 $\alpha(a, d) \leqq \alpha(a, b)$ $(d \in [b, a])$ holds, thus the elements $\alpha(a, d)$ belong to the interval $[a_0, \alpha(a, b)]$. Hence it is sufficient to prove that to every element d' $(\in [a_0, \alpha(a, b)])$ there belongs an element d $(\in [b, a])$ such that $d' = \alpha(a, d)$

holds. Let $d=\alpha(a,d')$ be an element belonging to an arbitrary element d' ($\in[a_0,\alpha(a,b)]$). Using condition c) we get

$$\alpha(a,d)=\alpha(a,\alpha(a,d'))=d'.$$

We show that $d\in[b,a]$ holds. Since $d=\alpha(a,d')$, so by condition a) $d\leqq a$ is valid. Since $d'\leqq\alpha(a,b)$, therefore by Property 2 we have

$$\alpha(a,d')\geqq\alpha(a,\alpha(a,b)),$$

that is

$$\alpha(a,\alpha(a,d))\geqq\alpha(a,\alpha(a,b)).$$

Applying condition c) to both sides we get $d\geqq b$. Thus Property 5 is proved.

Property 6. The correspondence $d\longleftrightarrow\alpha(d,b)$ is a one-to-one mapping between the elements of $[b,a]$ and $[a_0,\alpha(a,b)]$.

Namely, condition b) implies $\alpha(d,b)\in[a_0,a(a,b)]$. Hence it is sufficient to prove that every element d' ($\in[a_0,\alpha(a,b)]$) may be represented uniquely in the form $d'=\alpha(d,b)$ ($d\in[b,a]$). Let d' be an arbitrary element of the interval $[a_0,\alpha(a,b)]$. By Property 5 the elements d' are of the form $\alpha(a,d^*)$ where d^* is a uniquely determined element of the interval $[b,a]$. Using condition d) we get

$$d'=\alpha(a,d^*)=\alpha(\alpha(a,\alpha(d^*,b)),\alpha(d^*,\alpha(d^*,b))).$$

Using condition c) on the right-hand side, we get

$$d'=\alpha(\alpha(a,\alpha(d^*,b)),b),$$

i. e. $d'=\alpha(d,b)$, where $d=\alpha(a,\alpha(d^*,b))$. Like d^*, d is uniquely determined too. Since by condition a) $d=\alpha(a,\alpha(d^*,b))\leqq a$ holds, so by conditions c) and b) we have

$$b=\alpha(d^*,\alpha(d^*,b))\leqq\alpha(a,\alpha(d^*,b))=d,$$

therefore $d\in[b,a]$ is valid, proving the statement.

We return now to the proof of Theorem 4. Assume that α is an arbitrary factor-function. First we prove that the α-product is commutative. Consider the product

$$f\overset{\circ}{\alpha}g=\sum_{d\leqq a}f(d)\,g(\alpha(a,d)).$$

Since according to Property 5 each element $d(\leqq a)$ may be uniquely represented in the form $d=\alpha(a,d')$ ($d'\leqq a$) and since d' ranges over the interval $[a_0,a]$ too, so we get

$$f\overset{\circ}{\alpha}g=\sum_{d'\leqq a}f(\alpha(a,d'))\,g(\alpha(a,\alpha(a,d'))).$$

Using condition c) we get

$$f \overset{\circ}{\alpha} g = \sum_{d' \leqq a} f(\alpha(a, d'))\, g(d') = g \overset{\circ}{\alpha} f,$$

which proves the commutativity of the α-product.

Next we prove that the α-product is associative. Let f, g, h be arbitrary functions of $\mathfrak{F}$. Consider the α-product

$$f \overset{\circ}{\alpha} (g \overset{\circ}{\alpha} h) = \sum_{d \leqq a} f(d) \sum_{d^* \leqq \alpha(a, d)} g(d^*)\, h(\alpha(\alpha(a, d), d^*)). \tag{7}$$

By Property 6 d^* is of the form $d^* = \alpha(d', d)$, where d' is a uniquely determined element of the interval $[d, a]$, which ranges over the interval $[d, a]$ when d^* ranges over the interval $[a_0, \alpha(a, d)]$. Taking this into consideration, transform the right-hand side of (7). We get

$$f \overset{\circ}{\alpha} (g \overset{\circ}{\alpha} h) = \sum_{d \leqq a} f(d) \sum_{d \leqq d' \leqq a} g(\alpha(d', d))\, h(\alpha(\alpha(a, d), \alpha(d', d))).$$

Applying condition d) to the variable of the function h, we get

$$f \overset{\circ}{\alpha} (g \overset{\circ}{\alpha} h) = \sum_{d \leqq a} f(d) \sum_{d \leqq d' \leqq a} g(\alpha(d', d))\, h(\alpha(a, d')).$$

Changing the summation variables, we can write

$$f \overset{\circ}{\alpha} (g \overset{\circ}{\alpha} h) = \sum_{d' \leqq a} \Big[\sum_{d \leqq d'} f(d)\, g(\alpha(d', d))\Big]\, h(\alpha(a, d')) = (f \overset{\circ}{\alpha} g) \overset{\circ}{\alpha} h.$$

This proves the associativity of the α-product.

We show that the Dirac function δ is the identity of $\mathfrak{F}$ with respect to the α-product. Namely, since $\delta(a)$ is zero unless a is a minimal element of S, so by Property 4 we have

$$\delta \overset{\circ}{\alpha} f = \sum_{d \leqq a} \delta(d)\, f(\alpha(a, d)) = \delta(a_0)\, f(\alpha(a, a_0)) = f(a).$$

Thus we have proved the necessity of the condition.

Suppose, conversely, that the α-product is commutative and associative. By the commutativity we have $f \overset{\circ}{\alpha} g = g \overset{\circ}{\alpha} f$, i. e.

$$\sum_{d \leqq a} f(d)\, g(\alpha(a, d)) = \sum_{d' \leqq a} g(d')\, f(\alpha(a, d')).$$

Since this is true for any two functions $f, g\ (\in \mathfrak{F})$, therefore to each element $d\ (\leqq a)$ there corresponds an element $d'\ (\leqq a)$ such that $d = \alpha(a, d')$ and $d' = \alpha(a, d)$ are valid at the same time. Substituting d' into the expression of d, we get $d = \alpha(a, \alpha(a, d))$ which means just that condition c) holds. Since $\alpha(a, d) = d' \leqq a$, so condition a) holds too.

By the associativity, for any $f, g, h\,(\in \mathfrak{F})$ the equation $f \overset{\circ}{\alpha} (g \overset{\circ}{\alpha} h) = (f \overset{\circ}{\alpha} g) \overset{\circ}{\alpha} h$ is valid, i.e. we have

$$(8)\ \sum_{d \leqq a} f(d) \sum_{d^* \leqq \alpha(a,d)} g(d^*)\, h(\alpha(\alpha(a,d), d^*)) = \sum_{d' \leqq a} \sum_{d \leqq d'} f(d)\, g(\alpha(d', d))\, h(\alpha(a, d')).$$

Compare the variables of the function g. Equation (8) holds for any $f, g, h\,(\in \mathfrak{F})$ only if the set of the elements $\alpha(d', d)$ $(d \leqq d' \leqq a)$ coincides with the set of the elements d^* $(\leqq \alpha(a, d))$ and to every element d^* $(\leqq \alpha(a, d))$ there corresponds a single element d' $(\in [d, a])$ such that $d^* = \alpha(d', d)$ is valid. Obviously, in the case $d' < a$ the relation

$$\alpha(d' d) < \alpha(a, d)$$

holds, which implies condition b).

Compare the variables of the function h. Equation (8) holds only if

$$\alpha(\alpha(a, d), d^*) = \alpha(a, d')$$

is valid. Since by the previous facts $d^* = \alpha(d', d)$, so the equation

$$\alpha(\alpha(a, d), \alpha(d', d)) = \alpha(a, d')$$

holds, which implies condition d). Hence the proof is finished.

In the sequel denote by α an arbitrary function of two variables. We shall determine the functions which have a so-called left-α-inverse.

Theorem 5. *If f is any function $\in \mathfrak{F}$ and a is an arbitrary element of S such that $f(\alpha(a, a))$ is not zero, then there exists a function f_α^{-1} such that the equation*

$$(9)\qquad f_\alpha^{-1} \overset{\circ}{\alpha} f = \delta(a)$$

holds.

Proof. Let a be a minimal element of S. Now we can write (9) in the form

$$f_\alpha^{-1}(a)\, f(\alpha(a, a)) = 1.$$

Since $f(\alpha(a, a)) \neq 0$, so in this case $f_\alpha^{-1}(a)$ is uniquely determined.

Now let a be an arbitrary but not minimal element of S and assume that the statement is true for the elements d less than a. Now (9) has the form

$$\sum_{d \leqq a} f_\alpha^{-1}(d)\, f(\alpha(a, d)) = 0,$$

that is

$$\sum_{d < a} f_\alpha^{-1}(d)\, f(\alpha(a, d)) + f_\alpha^{-1}(a)\, f(\alpha(a, a)) = 0.$$

This equation determines $f_\alpha^{-1}(a)$ uniquely and this completes the proof.

Let α denote an arbitrary factor-function. The next theorem is a trivial consequence of Theorems 4 and 5.

Theorem 6. *If* $f \overset{\circ}{\alpha} g = F(a)$ $(f, g, F \in \mathfrak{F};\ g(\alpha(a,a)) \neq 0)$, *then* $f(a) = F \overset{\circ}{\alpha} g_\alpha^{-1}$.

Let ε denote the function $\varepsilon(a) = 1$ $(a \in S)$. It is easy to see that the function ε is exactly the α-inverse of the Möbius function (and vice versa). In particular for $g = \varepsilon$ we get

$$f(a) = F \overset{\circ}{\alpha} \mu, \tag{10}$$

which is exactly the Möbius inversion formula. Equation (10) shows that $f(a)$ is a linear expression of the values of $F(d)$ $(d \leqq a)$, with coefficients which are the values of the Möbius function. So by Theorem 2 the factor-function α satisfies condition (4). Hence we have proved

Theorem 7. *Every factor-function* α *satisfies condition* (4), *i. e. the equation*

$$\sum_{b \leqq d \leqq a} \mu(\alpha(d, b)) = \begin{cases} 1 & \text{if } b = a, \\ 0 & \text{otherwise} \end{cases}$$

holds.

It is easy to prove Theorem 7 immediately. Namely, by Property 6 the elements $d' = \alpha(d, b)$ $(d \in [b, a])$ form the interval $[a_0, \alpha(a, b)]$, thus according to the definition of the Möbius function

$$\sum_{b \leqq d \leqq a} \mu(\alpha(d, b)) = \sum_{d' \leqq \alpha(a, b)} \mu(d') = \begin{cases} 1 & \text{if } b = a, \\ 0 & \text{otherwise} \end{cases}$$

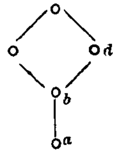
is valid.

It happens that more factor-functions may be defined on a given set. We can see this easily on the example of the modular lattice of order five. There are sets on which we can not define any factor-function, but there exists a function satisfying condition (4).

Example 3. Consider the set $S_3 = \{a, b, c, d, e\}$ with the partial ordering

$$a < b < c < e, \quad a < b < d < e.$$

The diagram of S_3 is the following:



We show that we can not define any factor-function on S_3 Suppose that α

is a factor-function defined on S_8 Now the relations

$$a=\alpha(e,e)<\alpha(e,c)<\alpha(e,b)<\alpha(e,a)=e,$$
$$a=\alpha(e,e)<\alpha(e,d)<\alpha(e,b)<\alpha(e,a)=e$$

are valid. The relations of S_8 and these imply $\alpha(e,c)=\alpha(e,d)$, and so Property 1 implies $c=d$ which is a contradiction.

It is easy to see that any function f defined on S_8 may be expressed by its sum function as follows:

$$f(a)=F(a),$$
$$f(b)=F(b)-F(a),$$
$$f(c)=F(c)-F(b)+0\cdot F(a),$$
$$f(d)=F(d)-F(b)+0\cdot F(a),$$
$$f(e)=F(e)-F(c)-F(d)+0\cdot F(b)+0\cdot F(a),$$

and the values of the Möbius function are

$$\mu(a)=1,\quad \mu(b)=-1,\quad \mu(c)=\mu(d)=\mu(e)=0.$$

Since the coefficients of the values of F are exactly the values of the Möbius function, so we can define a function on S which fulfils condition (4).

4. The theory of Delsarte

1. Let $C_k\,(k=1,2,\ldots)$ be groups which are isomorphic to the group of all complex roots of unity, or otherwise expressed, to the group of all finite rotations of the circle. Clearly each C_k is the discrete direct product of quasicyclic groups belonging to the distinct primes. Consider the discrete direct product of the groups $C_k\,(k=1,2,\ldots)$, and denote this group by A. Let S_A be the set of the finite subgroups of A. Clearly the elements of S_A are Abelian groups, and every finite Abelian group is isomorphic to any (or more) elements of the set S_A. Denote the inclusion of groups by the sign $\leqq$. Under the relation of inclusion the set S_A is partially ordered. Define the function β of two variables on S_A as follows.

i) If $b\not\leqq a$ $(a,b\in S_A)$, then $\beta(a,b)$ means the identity.

ii) If a $(\in S_A)$ is a cyclic group of order p^n and b is a subgroup of order p^k $(k\leqq n)$ in a then $\beta(a,b)$ means the subgroup of order p^{n-k} in a.

iii) Let a,b $(b\leqq a\in S_A)$ be arbitrary groups. Let $b=\prod_{i=1}^{n} b_i$ be any decomposition of b into the direct product of cyclic groups of prime power order. Obviously the group a may be decomposed into the direct product of cyclic groups of prime power order in the form $a=\prod_{i=1}^{N} a_i$ such that $b_i \leqq a_i$ $(i=1, \ldots, n)$ hold. Now let $\beta(a, b)$ mean the direct product of the groups $\beta(a_i, b_i)$ $(i=1, \ldots, n)$ and a_i $(i=n+1, \ldots, N)$, i. e.

$$\beta(a, b)=\prod_{i=1}^{n} \beta(a_i, b_i) \prod_{i=n+1}^{N} a_i .$$

We show that the function β is a factor-function. In the cases i), ii) the function β fulfils conditions a), b), c) and d) trivially. In the case iii) β satisfies conditions a) and b) obviously. Since

$$\beta(a, \beta(a, b))=\beta\left(\prod_{i=1}^{N} a_i, \prod_{i=1}^{n} \beta(a_i, b_i) \prod_{i=n+1}^{N} a_i\right)=$$

$$=\prod_{i=1}^{n} \beta(a_i, \beta(a_i, b_i)) \prod_{i=n+1}^{N} \beta(a_i, a_i)=\prod_{i=1}^{n} b_i=b,$$

so condition c) is fulfilled. Let a, b, c $(c \leqq b \leqq a \in S_A)$ be three arbitrary groups and let

$$c=\prod_{i=1}^{k} c_i, \quad b=\prod_{i=1}^{l} b_i, \quad a=\prod_{i=1}^{n} a_i$$

be their decompositions into cyclic groups of prime power order such that $c_i \leqq b_i$ $(i=1, \ldots, k)$ and $b_i \leqq a_i$ $(i=1, \ldots, l)$ hold. Clearly this is possible. Since in the case ii) condition d) is fulfilled therefore we have

$$\beta(\beta(a, c), \beta(b, c))=\beta\left(\prod_{i=1}^{k} \beta(a_i, c_i) \prod_{i=k+1}^{n} a_i, \prod_{i=1}^{k} \beta(b_i, c_i) \prod_{i=k+1}^{l} b_i\right)=$$

$$=\prod_{i=1}^{k} \beta(\beta(a_i, c_i), \beta(b_i, c_i)) \prod_{i=k+1}^{l} \beta(a_i, b_i) \prod_{i=l+1}^{n} a_i=$$

$$=\prod_{i=1}^{k} \beta(a_i, b_i) \prod_{i=k+1}^{l} \beta(a_i, b_i) \prod_{i=l+1}^{n} a_i=\beta(a, b).$$

Hence we proved that condition d) is satisfied, and so β is a factor-function.

Since β is a factor-function, so the results of section 3 are true for complex-valued functions defined on S_A. If we consider only functions f such that $f(a)=f(b)$ if a, b $(\in S_A)$ are isomorphic, we get exactly the results of DELSARTE. In this case namely we can define the functions f for every finite Abelian group by the equations

$$f(g_a)=f(a) \qquad (g_a \approx a;\ a \in S_A)$$

where g_a means an arbitrary finite Abelian group. Since by ii) and iii)

$\beta(a, b)$ $(b \leqq a \in S_A)$ are isomorphic to the factor group a/b, so the β-product of any two functions f, g has the form

$$f \overset{\circ}{\beta} g = \sum_{d \leqq a} f(a)\, g(a/d),$$

which is exactly the Möbius product defined by DELSARTE.

Consider now the group C_k for a fixed positive integer k, and denote the set of the finite subgroups of C_k by S_C. Clearly the inclusion $S_C \subseteqq S_A$ holds, and the elements of S_C are finite cyclic groups. In this special case of DELSARTE's theory we get the classical number-theoretic Möbius function and inversion formula.

2. We may get the number-theoretic Möbius function and inversion formula in another way too. Consider namely the ideals of the ring I of the integers, except for the zero-ideal. Denote the set of these ideals by S_I. Every element of S_I is a principal ideal $\{n\}$ where n means any positive integer. Denote the fact that the ideal $\{d\}$ contains the ideal $\{n\}$ by $\{d\} \leqq \{n\}$ (i. e. the integer d divides n). Thus S_I becames a partially ordered set, and since S_I does not contain the zero-ideal, so every relation $\{x\} \leqq \{n\}$ has only a finite number of solutions for any fixed n. Define the function β of two variables on S_I as follows:

$$\beta(\{n\}, \{d\}) = \begin{cases} \left\{\dfrac{n}{d}\right\} & \text{if } \{d\} \leqq \{n\}, \\ \{1\} & \text{otherwise.} \end{cases}$$

It is easy to see that the function β satisfies conditions a), b), c) and d), so β is a factor-function. If we apply the results of section 3 to complex-valued functions defined on S_I, then we get again the number-theoretic Möbius function and inversion formula.

We can get similar results as in DELSARTE's theory, if we form the discrete direct sum J of rings I_k $(k = 1, 2, \ldots;$ each I_k being isomorphic to the ring of integers), and apply the results of section 3 to the set of the ideals of J.

5. Möbius inversion formula on a set of subsets

Let M be an arbitrary countable set, and let S_M be the set of the finite subsets of M. In the sequel let s_n $(\in S_M)$ denote any set of n elements. Let $\gamma(s_n, s_k)$ mean the complement of s_k in s_n if the inclusion $s_k \subseteqq s_n$ holds, and the void-set otherwise. γ fulfils condition a), b) and c) trivially.

We show that γ is a factor-function. It is sufficient to prove that condition d) holds. For this aim let $s_l, s_k, s_n (\in S_M)$ be arbitrary sets satisfying the inclusion $s_l \subseteqq s_k \subseteqq s_n$. The set $s_x = \gamma(\gamma(s_n, s_l), \gamma(s_k, s_l))$ consists of the elements which belong to s_n, but neither to s_l nor to the complement of s_l in s_k. Since $s_l \subseteqq s_k$ holds, so the set s_x consists exactly of the elements of the complement of s_k in s_n, i. e. $s_x = \gamma(s_n, s_k)$. This proves our statement.

Theorem 8. *If μ means the Möbius function defined on S_M, and $s_n (\in S_M)$ is an arbitrary set of n elements, then $\mu(s_n) = (-1)^n$.*

Proof. For $n=0$ the assertion is obvious. Assume it is true for the integers k less than n. By the definition of the Möbius function for any positive integer n, we have

$$\sum_{s_k \subseteqq s_n} \mu(s_k) = 0,$$

i. e.

$$\sum_{s_k \subset s_n} \mu(s_k) + \mu(s_n) = 0.$$

By the induction hypothesis we have

$$\sum_{s_k \subset s_n} (-1)^k + \mu(s_n) = 0.$$

Since a set of n elements has $\binom{n}{k}$ subsets of k elements, so we can write the left-hand side in the form

$$\sum_{k=0}^{n-1} \binom{n}{k} (-1)^k + \mu(s_n) = 0.$$

Adding $(-1)^n$ to both sides we get

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k + \mu(s_n) = (-1)^n.$$

Since $\sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$, therefore $\mu(s_n) = (-1)^n$ which completes the proof.

Theorem 9. *Let $f(n)$ be any function defined for non-negative integers and its values belong to a given module. If F is the function defined by the equation*

$$\sum_{k=0}^{n} \binom{n}{k} f(k) = F(n), \tag{11}$$

then

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} F(k) = f(n) \tag{12}$$

is true.

Proof. Define the functions f and F on the set S_M by the equations

$$f(s_n)=f(n) \quad \text{and} \quad F(s_n)=F(n) \qquad (s_n \in S_M).$$

Hence according to Theorem 8 we can write equations (11) and (12) in the form

$$\sum_{s_k \subseteqq s_n} f(s_k)=F(s_n),$$

$$\sum_{s_k \subseteqq s_n} \mu(\gamma(s_n, s_k))\, F(s_k)=f(s_n).$$

By Theorem 3 these equations are equivalent, proving our statement.

Theorem 10. *Let $f(n)$ be any complex-valued function defined for non-negative integers. Define the function $F(n)$ recursively, by the equations*

$$F(0)=f(0),$$

$$F(n)=f(n)+anf(n-1) \quad (n>0,\ a \text{ a complex number}).$$

Then f is determined uniquely by F and the equation

$$\sum_{k=0}^{n} \frac{n!}{k!}(-1)^{n-k} a^{n-k} F(k)=f(n)$$

is valid.

Proof. Define the functions f, F on S_M by the equations

$$f(s_n)=f(n), \quad F(s_n)=F(n) \qquad (s_n \in S_M).$$

Let ξ denote the function

$$\xi(s_n)=\xi(n)=\begin{cases} 1 & \text{if } n=0, \\ a & \text{if } n=1, \\ 0 & \text{otherwise.} \end{cases}$$

Consider the product $\xi \overset{\circ}{\gamma} f$, i. e.

$$\xi \overset{\circ}{\gamma} f=f(n)+anf(n-1)=F(n).$$

Since $\xi(0)$ is not equal to zero, thus by Theorem 6 the equation

$$F \overset{\circ}{\gamma} \xi_\gamma^{-1}=f \tag{13}$$

holds. Our purpose is to determine the function ξ_γ^{-1}. We show that $\xi_\gamma^{-1}= =(-1)^n a^n n!$ holds. This statement is true for $n=0$. Assume it is true for the integers less than n (>0). By the definition of the γ-inverse we have $\xi_\gamma^{-1} \overset{\circ}{\gamma} \xi=\delta$, i. e. in the case $n>0$

$$an\xi_\gamma^{-1}(n-1)+\xi_\gamma^{-1}(n)=0.$$

Using the induction hypothesis for $\xi_\gamma^{-1}(n-1)$ we get

$$(-1)^{n-1} a^n n!+\xi_\gamma^{-1}(n)=0,$$

which proves the statement. Now the equation (13) is of the form

$$\sum_{k=0}^{n} \frac{n!}{k!\,(n-k)!}(-1)^{n-k} a^{n-k}(n-k)!\,F(k)=f(n),$$

i. e.

$$\sum_{k=0}^{n} \frac{n!}{k!}(-1)^{n-k} a^{n-k} F(k)=f(n),$$

and this completes the proof.

Now we give a simple application of Theorem 10.

Example 4. Let f be the function $f(n)=n$, and let $a=1$. Now for the function F occurring in Theorem 10 we get

$$F(n)=n+n(n-1)=n^2.$$

Hence by Theorem 10 the equation

$$\sum_{k=0}^{n} \frac{n!}{k!}(-1)^{n-k} k^2=n$$

holds. Divide both sides by $n!$ and write $l+1$ instead of k. It results

$$\sum_{l=0}^{n-1} \frac{l+1}{l!}(-1)^{n-(l+1)}=\frac{1}{(n-1)!}.$$

Write N instead of $n-1$. We get the formula

$$\sum_{l=0}^{N} \frac{l+1}{l!}(-1)^{N-l}=\frac{1}{N!}.$$

Bibliography

[1] S. Delsarte, Fonctions de Möbius sur les groupes Abeliens finis, *Annals of Math.*, 49 (1948), 600—609.
[2] L. Rédei, Zetafunktionen in der Algebra, *Acta Math. Acad. Sci. Hung.*, 6 (1955), 5—25.
[3] L. Rédei, *Algebra* I (Leipzig, 1959).
[4] M. Ward, The algebra of lattice functions, *Duke Math. Journal*, 5 (1939), 357—371.
[5] L. Weisner, Abstract theory of inversion of finite series, *Transactions American Math. Soc.*, 38 (1935), 474—484.

(Received April 13, 1959)